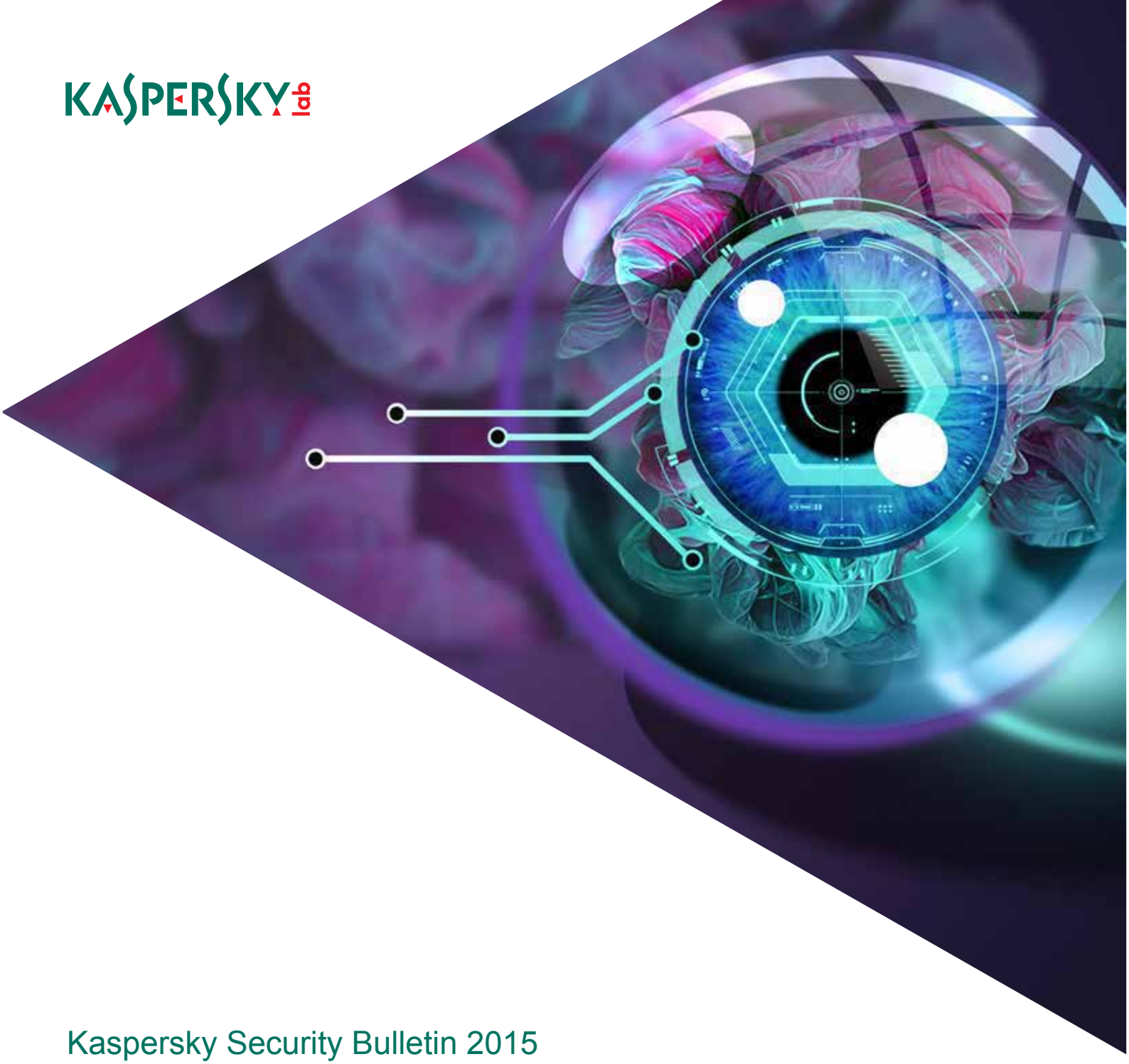
KASPERSKY lab



Kaspersky Security Bulletin 2015

2016年サイバー犯罪の予測：
APTは新たな形態へ

GREAT

目次

はじめに

2015年も残すところわずかとなりました。この1年のITセキュリティ業界の進化を評価するとともに、来年の動向を予測する時期です。Kaspersky LabのGlobal Research and Analysis Team（GReAT）とアンチマルウェアリサーチ部によるグローバルミーティングでは、世界中のエキスパートが一堂に会する貴重な機会を活かし、さまざまな意見が議論されました。2016年とその先の長期にわたる予測の中で、特に信憑性が高く注目すべきものを選んで紹介します。急速に進化するこの研究分野においては、将来の見通しを立てるにあたって考えさせられることが非常に多く、今後も興味深い課題が提示され続けることでしょう。厳格な基準を遵守することにより、SF的な恐怖で煽るありふれたマーケティングではなく、短期と長期の両方について正確な予測を導き出せるものと考えています。

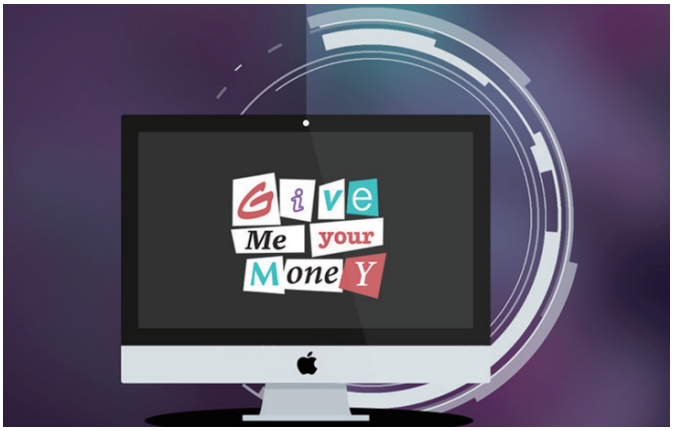
APTの終焉

期待させるようなことを書いてしまいましたが、終わりを迎えるのはAdvanced Persistent Threatの「Advanced」（高度）と「Persistent」（執拗）という要素です。いずれも、存在を覚られずに活動するためなら、APTグループが喜んで手放すものでしょう。今後は何度も繰り返される執拗な攻撃から、メモリ常駐型、つまりファイルレスのマルウェアに軸足が移っていくものと予測します。これは、感染システムに残る痕跡を減らし、検知を回避するためです。また、高度なマルウェアにかける比重を減らしていくというアプローチもとられるでしょう。さまざまなリサーチグループにより調査しつくされたブートキット、ルートキット、カスタムマルウェアに投資するのではなく、容易に入手できるマルウェアの転用が増えると考えられます。このアプローチには、発見されてもマルウェアプラットフォームの崩壊を免れられるというメリットだけでなく、広く利用されているRAT（Remote Acccess Tool）の中に、組織の存在とその意図を隠匿できるという付加価値もあります。サイバー能力の輝きが失われる中、国家による支援を受けた攻撃者の意思決定は、投資利益率（ROI）に大きく左右されることになるでしょう。初期投資を抑えること以上に、ROIの最大化に有効な手段はありません。

※ Global Research & Analysis Team（グローバル調査分析チーム、GReAT:グレート）
GReATはKaspersky Labで研究開発に携わる中核部門として、脅威に関する情報収集、調査研究およびその成果発表などの活動を通じ、社内および業界をリードしています。また、マルウェアによるインシデント発生時の対応措置を担当しています。

ランサムウェアの悪夢は続く

ランサムウェアの成功は、新たな領域に広がっていくものと思われます。従来のバンキング型マルウェアにないランサムウェアの利点として、利益を直接得られること、標的あたりのコストが比較的低いことの2つが挙げられます。これは、銀行など資金力のある第三者組織の関心の低下、そして警察機関への通報の減少につながります。Kaspersky Labでは、ランサムウェアがバンキング型トロイの木馬に追い迫るだけでなく、他のプラットフォームへ移行すると予測しています。ランサムウェアをモバイル（Simplelocker）やLinux（Linux.Encode.1）に感染させる試みもすでに数件確認されていますが、標的としてさらに価値の高いプラットフォームはおそらくOS Xでしょう。ランサムウェアを利用する犯罪者が重大な決断を下し、Macを標的とするだけではなく、「Mac価格」を請求してくると予測されます。その後、長期的にはIoTランサムウェアが登場する可能性もあります。つまり、テレビ、冷蔵庫、自動車をもう一度使えるようにするために、いくら払う用意があるかを問われるようになるのです。



金融犯罪が最高レベルに

サイバー犯罪とAPTの融合に勢いづいた金銭目的の犯罪者は、攻撃の矛先をエンドユーザーから金融機関に変えました。過去1年間で、POSシステムやATMに対する攻撃の例が多数確認されています。何億ドルもの金額を盗んだ大胆不敵なCarbanakはいうまでもありません。同様に、サイバー犯罪者は代替決済手段（Apple PayやAndroid Pay）のような目新しいものに狙いを定めると予想されます。こうした決済システムの普及が進むにつれ、容易に利益を得るための新たな手口が登場するでしょう。また、真の金脈とも言える証券取引所が標的となるのも避けられません。正面攻撃は短期間で利益を得られる可能性があるものの、目立たない手段での侵害の可能性も見逃せません。たとえば、逮捕される可能性を下げつつ、長期間にわたって利益を確保するために、高頻度取引に採用されているブラックボックスアルゴリズムを狙うといった手口です。

セキュリティベンダーに対する攻撃

セキュリティベンダーに対する攻撃が増加する中、業界標準のリバースエンジニアリングツール（IDAやHiewなど）、デバッグツール（OllyDbg、WinDbgなど）、仮想化ツール（VMwareスイート、VirtualBoxなど）の侵害という興味深いベクトルが予測されます。Linuxの‘strings’の実装に潜む脆弱性CVE-2014-8485は、重要なセキュリティリサーチツールの脆弱な現状を示す例です。リサーチャーをターゲットにすると決断した攻撃者は、この脆弱性の悪用を選択することがあります。同様に、GitHubのようなコードリポジトリでフリーウェアのリサーチツールを共有することは、乱用につながります。多くのユーザーは無警戒にコードを取得して自分のシステムで実行するためです。おそらく、情報セキュリティのコミュニティで幅広く採用されているPGP実装にも疑いの目を向ける必要があります。

妨害工作、恐喝、不名誉

有名人のヌード写真の流出から、ソニーやアシュレイ・マディソン（Ashley Madison）のハッキング、HackingTeam社からの漏洩まで、情報暴露、晒し上げ、恐喝が増加していることに疑いの余地はありません。ハクティビスト、犯罪者、国家支援の攻撃者は一様に、プライベート写真、情報、顧客リストやコードを戦略的に漏洩させ、標的にダメージを与えています。このような攻撃の中には戦略的に標的を設定しているものもありますが、一部は日和見主義の産物で、高度な技術を持つハッカーを装い、貧弱なサイバーセキュリティにつけ込んでいます。残念ながら、こうした活動は飛躍的に増加し続けていくでしょう。

誰を信じればいいのか

今のインターネット時代に最も不足しているのは信頼かもしれません。信頼されたリソースの悪用は、この不足に拍車をかけます。攻撃者は、オープンソースライブラリや、ホワイトリストに登録されたリソースを悪意に満ちた目的で登用し続けるでしょう。Kaspersky Labでは、別の形の信頼が悪用されると予想しています。それは企業の社内リソースの信頼です。狡猾な攻撃者は、感染したネットワークでの足掛かりを拡大するため、SharePoint、ファイルサーバーやADPポータルへの水飲み場型攻撃など、企業のイントラネットに限定されたリソースを標的にする可能性があります。攻撃者が偽の証明機関を一から立ち上げ、自分たちのマルウェアに証明書を発行するにつれて、すでに蔓延している信頼済み証明書の悪用がさらに拡大していく恐れもあります。

APTグループの今後

サイバースパイ活動による利益を、犯罪者が見逃すことはありませんでした。予想どおり、サイバー傭兵たちがこの分野に集まり始めています。このトレンドは拡大の一途を辿るでしょう。一部の企業や既知のAPTグループは、自らのツールやインフラストラクチャを危険にさらすことなく、重要度の低いタスクをアウトソースする方法を模索しており、こうした組織が外部のサイバー能力を求めているためです。新しい用語として「APT-as-a-Service」を今回提案することもできましたが、それよりもさらに興味深いのは、標的型攻撃が進化して「Access-as-a-Service」を提供するようになるという予測かもしれません。後者には、すでにサイバー傭兵の被害に遭った著名組織へのアクセス権の販売も含まれます。

さらに先のサイバースパイ活動について考えてみると、有力なAPTグループのメンバー（いうなればAPTの上位1%）が舞台裏から姿を現す可能性が見えてきます。これには2つの形態が考えられます。1つは、「報復ハッキング」の蔓延に伴い、民間企業に荷担するという形です。もう1つは、大規模な情報セキュリティコミュニティと知見を共有する形です。この場合、APTメンバーがセキュリティカンファレンスに参加して、サイバースパイ活動をAPTグループの立場から語ることになるでしょう。そうなるまでに、APTというバベルの塔にさらに数か国語が取り入れられるものと予測されます。

インターネットの未来

近年、インターネット自体のインフラストラクチャに緊張や亀裂の兆候が見られます。大規模なルーターボットネット、BGPの乗っ取りや情報漏洩、一斉DNS攻撃、サーバーによるDDoSに対する懸念は、説明責任と法執行の世界規模での欠如を表しています。さらに先を見て、長期的な予測を立てるのは、この世界的に接続された村という物語が縮小を続けた場合に、インターネットがどうなるかを考えることです。インターネットが国境で細かく分断されてしまう可能性もあります。その時点では、可用性に関する懸念は、セクション間にアクセスを提供するサービス接合点への攻撃、あるいは、インターネットの大部分を接続するケーブルを標的とした地政学的な緊張関係に集約されるかもしれません。おそらく、接続を扱うブラックマーケットも登場するでしょう。同様に、インターネットの弱点を強化する技術が大きな注目を集め、採用が広がり続けるにつれて、闇の市場や為替レート、フォーラムとの関係を持つ開発者が、地下社会を文字どおり地下に閉じ込めておくための優れた技術を開発するはずです。

交通の未来

投資やハイエンドのリサーチ機能が、自家用と商用の両分野で自動運転車の開発に向けられるなか、このような乗り物が大量に走行するルートやトラフィックを管理するための交通システムが発展することになるでしょう。交通システム自体は攻撃の対象とならないかもしれませんが、これらのシステムが依存しているプロトコルの妨害やなりすましが行われると考えられます（広く採用されているGlobal Star衛星通信システムの脆弱性の概念実証は、今年のBlackHatカンファレンスで、Synackのリサーチャーが講演しました）。このような攻撃の陰に潜む目的は、高額商品の窃盗や人命の喪失につながる動力学的な被害と見られます。

暗号の終焉は近い

最後になりますが、比べるものがないほど有望な情報共有とトランザクションツールとして、インターネットの機能的価値を維持するためには、暗号化標準の重要性をいくら強調してもしすぎることはありません。このような暗号化標準は、暗号化された出力を解読するために必要な計算能力が、種としての人間の英知を超えるものであるという前提に立ってしています。しかし、将来、量子コンピューターの進歩が約束しているとおり、コンピューターの計算能力が飛躍的に前進したときには何が起こるでしょうか。一般的なサイバー犯罪者は初めのうち、量子機能を利用できないでしょう。しかし、これは現在の暗号化標準に対する信頼性の崩壊と、「ポスト量子暗号」の設計および実装の必要性を示唆しています。高品質の暗号の採用や適切な実装が遅々として進まない現状に照らせば、大きな規模で暗号化の失敗を相殺すべくスムーズな移行が実施されるとは考えられません。

株式会社カスペルスキー
PR-1019-201512